REMARKS

Claims 2-17 are pending and were examined. Claims 2-17 were rejected under 35 U.S.C. §112, first and second paragraphs. Claims 2-7, 9, 11-13 and 16 were rejected under, 35 U.S.C. §102. Claims 8, 10, 14 and 15 were rejected under 35 U.S.C. §103. Claim 1 has been canceled in a previous amendment. Claims 9, 11 and 13 are currently amended. No new matter has been added. Accordingly, Claims 2-17 are presented for further examination.

Foreign Priority Claim Under 35 U.S.C. § 119(b)

The Examiner has acknowledged Applicant's claim for foreign priority based on German Application No. 199 19 909.4, filed April 30, 1999. However, the Examiner has requested a certified copy of the German Application pursuant to 35 U.S.C. § 119(b). Accordingly, the Applicant has enclosed hereto a certified copy of the above mentioned German application. The Applicant therefore requests that the Examiner establish the effective priority date for the present application as April 30, 1999.

Rejection under 35 U.S.C. §112, First Paragraph:

The Examiner rejects claims 9 and 11 under 35 U.S.C. §112, first paragraph, as allegedly failing to comply with the written description requirement. In support of the rejections, the Examiner alleges that the specification "fails short" of teaching "using the check key and the determined sequence number to form a calculated signature." Accordingly, the Applicant has amended claims 9 and 11 herein to clarify that the check key is derived from the determined sequence number. The Applicant asserts that the specification provides proper support for claims 9 and 11, as amended at least at page 6 lines 21-27 and FIG. 1. Thus, no new matter is presented. Accordingly, the Applicant respectfully requests that the rejections of claims 9 and 11 under 35 U.S.C. §112, first paragraph, be withdrawn.

The Examiner has rejected claim 13 under 35 U.S.C. §112, first paragraph, as allegedly failing to comply with the written description requirement. In support of the rejection, the Examiner states that even though the specification discloses "these pseudo-random number generators produce a sequence of new numbers in each case until the cycle..." that the specification "fails short" of disclosing that a new value is produced when a data set is received at the receiver. The Applicant respectfully disagrees and refers the Examiner to specification at page 7 lines 11-15, which reads as follows.

"Whenever a message is received, the receiver produces a new value for the sequence number, and thus forms the check key 14' without the sequence number having to be transmitted as well."

Furthermore, page 6 lines 13-17 of the specification establishes that message is part of the data set. Therefore, the data set is received when the message is received. The Applicant submits an amendment to claim 13 herein to clarify the step of receiving the data set and the receiver producing a new value of the sequence number. Proper support for claim 13 is found in the specification at least at page 7 lines 11-15 and page 6 lines 13-17. Thus, no new matter is presented. The Applicant therefore requests that the Examiner's rejection of claim 13 under 35 U.S.C. §112, first paragraph, be withdrawn.

The Examiner rejects claims 2-8, 12, 14-17 under 35 U.S.C. §112, first paragraph, as allegedly failing to comply with the written description requirement by virtue of their dependence on claims 9 and 11. Based on the foregoing, proper support for claims 9 and 11 is found in the specification. As such, the Examiner's rejections of claims 2-8, 12, 14-17 under 35 U.S.C. §112, first paragraph, is moot. Accordingly, the Applicant requests that the Examiner's rejections of claims 2-8, 12, 14-17 under 35 U.S.C. §112, first paragraph, be withdrawn.

Rejection under 35 U.S.C. §112, Second Paragraph:

The Examiner rejects claims 9 and 11 under 35 U.S.C. §112, second paragraph, as allegedly being indefinite. In support of the rejections, the Examiner alleges that the specification "fails short" of teaching "using the check key and the determined sequence number to form a calculated signature" and is therefore treated as the check key being used to derive the determined sequence number to form a calculated signature. Accordingly, the Applicant has amended claims 9 and 11 herein to clarify that the check key is derived from the determined sequence number. The Applicant asserts that the specification provides proper support for claims 9 and 11, as amended, at least at page 6 lines 21-27 and FIG. 1. Thus, no new matter is presented. The Applicant asserts that claims 9 and 11 therefore particularly point out and distinctly claim the subject matter regarded as the Applicant's invention.

In addition, the Examiner alleges that the step in claim 11 reciting "the sender using the at least one pair of the signing key and the selected sequence number to form a signature for a message" is indefinite and is therefore treated as "the sender using the at least one pair of the signing key and the selected sequence number to form a data set that contains a signature for a message." The Applicant respectfully refers the Examiner to page 5 lines 31-34 of the specification which reads as follows.

> "The sender 20 who wishes to send a message 21 to the receiver 30 takes a pair of sequence numbers 12 and signing keys 14 and uses the signer 24 to determine the signature for the message 21."

The above quoted phrase demonstrates that the step "the sender using the at least one pair of the signing key and the selected sequence number to form a signature for a message" recited in claim 11 particularly points out and distinctly claims the subject matter of the present invention. In addition, the step immediately following the step which the Examiner alleges is indefinite recites "the sender forming a data set." Support for this step is found in the specification at page 6 lines 8-10 which reads as follows.

> "The sender then forms a data set 22, which contains three fields with the sequence number 22a, the message 22b and the signature 22c."

The Applicant therefore disagrees with the Examiner's reading of the step in claim 11 reciting "the sender using the at least one pair of the signing key and the selected sequence number to form a signature for a message" in which the Examiner proposes to insert the term "a data set that contains" after the word "form." Based on the above, the step of forming a data set occurs after the forming of a signature for a message. Therefore, it is inappropriate to modify the step alleged to be indefinite as the Examiner suggests. Based on the above and with further reference to FIG. 1, the step in claim 11 reciting "the sender using the at least one pair of the signing key and the selected sequence number to form a signature for a message" particularly points out and distinctly claims the subject matter regarded as the Applicant's invention.

The Examiner also alleges that the step in claim 11 reciting "the check key and the determined sequence number being used to form a calculated signature for comparison to the signature of the data message block" is indefinite and is therefore treated as "the check key

and the determined sequence number being used to derive the check key that is used in forming a calculated signature for comparison to the signature of the data message block." The Examiner states that claim 9 is similarly rejected. Accordingly, the Applicant has amended claims 9 and 11 herein to clarify that the check key is derived from the determined sequence number. The Applicant concludes that claims 9 and 11 therefore, particularly point out and distinctly claim the subject matter regarded as the Applicant's invention.

The Examiner rejects claim 13 under 35 U.S.C. §112, second paragraph, as allegedly being indefinite. In support of the rejection, the Examiner alleges that it is not clear whether the limitation "when the data set is received at the receiver, producing a new value of the sequence number" is directed to the control center creating a new value of the sequence number. The Examiner also alleges that the meaning of the term "when" is not clear. Accordingly, the Applicant has amended claim 13 herein. The Applicant submits an amendment to claim 13 herein to clarify the step of receiving the data set and the receiver producing a new value of the sequence number. Proper support for claim 13 is found in the specification at least at page 7 lines 11-15 and page 6 lines 13-17. Thus, no new matter is presented. The Applicant concludes that claim 13 therefore particularly points out and distinctly claims the subject matter regarded as the Applicant's invention.

In view of the foregoing, the Applicant respectfully requests the Examiner to enter the proposed amendments to Claims 9, 11 and 13 and to reconsider and withdraw the rejections of Claims 9, 11 and 13 under 35 U.S.C. §112, second paragraph.

The Examiner rejects claims 2-8, 12, 14-17 under 35 U.S.C. §112, second paragraph, as allegedly being indefinite by virtue of their dependence on claims 9 and 11. Based on the foregoing claims 9 and 11 particularly point out and distinctly claim the subject matter regarded as the Applicant's invention. As such, the Examiner's rejections of claims 2-8, 12, 14-17 under 35 U.S.C. §112, second paragraph, are moot. Accordingly, the Applicant requests that the Examiner's rejections of claims 2-8, 12, 14-17 under 35 U.S.C. §112, second paragraph, be withdrawn.

Prior Art Rejections:

The Examiner rejects claims 2-7, 9 and 11-13 under 35 U.S.C. §102(b) as allegedly being anticipated by United States Patent No. 5,608,800 to Hoffmann et al (hereinafter the '800 reference). These rejections are respectfully disagreed with, and are traversed below.

In support of the rejection of claim 11, the Examiner alleges that the '800 reference discloses all the limitations of claim 11, including the signing key and the sequence number being provided by a control center to the sender. The Examiner alleges that a control center and a sender are both within a transmitter. Applicant respectfully disagrees with this characterization of the '800 reference.

The '800 reference is merely seen to disclose a process for detecting unauthorized introduction of data transmitted by a transmitter to a receiver. The process disclosed in the '800 reference includes a random data generator at the transmitter for generating random data to be used with coupling data to create a symmetric key.

However, without addressing the patentability of claim 11 as previously presented in view of the '800 reference and merely to streamline prosecution of the present application, clarifying amendments have been made to claim 11. Support for the proposed amendments to claim 11 may be found in the original disclosure at least at page 3, lines 16-18 and FIG. 1. Thus, no new matter is presented. These amendments to claim 11 have been discussed in a telecommunication between the Applicant's Attorney and the Examiner and subsequently e-mailed by Applicant's Attorney to the Examiner on January 4, 2006. Unlike claim 11 of the present application, the '800 reference does not disclose, teach or suggest all of the limitations of claim 11. For example, as now written claim 11 recites:

> "11. A method for signing a message from a sender and for checking a signature at a receiver, the method comprising the steps of: storing, in a control center and a receiver, a shared main key; causing the control center to produce one or more sequence numbers; using a selected one of the sequence numbers and the shared main key to create a signing key by means of a one-time encryption; providing at least one pair of the signing key and the selected sequence number to the sender via a secure transmission; the sender using the at least one pair of the signing key and the selected sequence number to form a signature for a message; the sender forming a data set; the sender sending the message to the receiver via the data set containing at least the message and the signature; determining, at the receiver, a sequence number for the received data set; passing the determined sequence number and the shared main key through a one-time encryption to produce a check key; using the check key that is derived from the determined sequence number to form a calculated signature; and comparing the calculated signature to the received signature to verify the received message; wherein the control center, the receiver, and the sender are individual and separate one from the other."

Since the '800 reference is not seen to disclose, teach or suggest, inter alia, the control center, the receiver, and the sender being individual and separate one from the other, it is respectfully submitted that the '800 reference fails to disclose or suggest the limitations of

claim 11 as now written. The Applicant therefore concludes that claim 11 is not anticipated by the '800 reference. Accordingly, the Applicant respectfully requests that rejection of claim 11 be reconsidered and withdrawn.

In support of the rejection of claim 9 the Examiner states that the limitations of claim 9 are substantially equivalent to the limitations of claim 11. The Examiner therefore states that claim 9 is "similarly rejected."

The deficiencies of the '800 reference have been discussed above. However, without addressing the patentability of claim 9 as previously presented in view of the '800 reference and merely to streamline prosecution of the present application, clarifying amendments have been made to claim 9, similar to those presented above for claim 11. Since the '800 reference is not seen to disclose, teach or suggest, inter alia, the control center, the receiver, and the sender being individual and separate one from the other, it is respectfully submitted that the '800 reference fails to disclose or suggest the limitations of claim 9 as now written. The Applicant therefore concludes that claim 9 is not anticipated by the '800 reference. Accordingly, the Applicant respectfully requests that rejection of claim 9 be reconsidered and withdrawn.

Claims 2-7, 12 and 13 depend directly or indirectly from claims 9 or 11. Because claims 9 and 11 are asserted to be patentable for the reasons presented above, dependant claims 2-7, 12 and 13 are necessarily patentable. Applicant, therefore, respectfully submits that claims 2-7, 12 and 13 are allowable. Accordingly, Applicant respectfully requests that the rejections of claims 2-7, 12 and 13 be reconsidered and withdrawn.

The Examiner rejects claim 8 under 35 U.S.C. §103(a) as being unpatentable over the '800 reference in view of U.S. Patent No. 6,009,401 to Horstmann (hereinafter the Horstmann reference). The Examiner states that the '800 reference does not disclose the receiver maintaining a list of already used sequence numbers and rejecting already used sequence numbers. However, the Examiner alleges that the Horstmann reference teaches a receiver maintaining a list of already used sequence numbers and rejects used sequence numbers. The Examiner further alleges that it would have been obvious for one of ordinary skill in the relevant art to modify the '800 reference to in view of the teachings of Horstmann to arrive at the invention of claim 8. These rejections are respectfully disagreed with, and are traversed below.

The deficiencies of the '800 reference is discussed above.

The Horstmann reference is merely seen to disclose a mechanism for use in electronic software distribution that provides purchase documentation and allows for re-download and re-licensing of software. The Horstmann reference discloses a clearinghouse keeping a list of used tickets to avoid replay attack. The clearinghouse of the Horstmann reference confirms that the ticket has not been previously used. Claim 8 depends directly from claim 11. Because claim 11 is asserted to be patentable for the reasons presented above, and because the Horstmann reference does not cure the deficiencies of the '800 reference, dependant claim 8 is necessarily non-obvious and therefore patentable. Applicant, therefore, submits that claim 8 is allowable. Accordingly, Applicant respectfully requests that the rejection of claim 8 be reconsidered and withdrawn.

The Examiner rejects claims 10 and 15 under 35 U.S.C. §103(a) as being unpatentable over the '800 reference in view of Official Notice. Regarding claim 10, the Examiner states that the '800 reference does not disclose the random generator producing a sequence number using a deterministic method. However, the Examiner alleges that it is old and well known to use deterministic methods to produce numbers. Regarding claim 15, the Examiner states that the '800 reference does not teach storing the signing key and selected sequence number in a smart card. However, the Examiner alleges that it is old and well-known practice to use smart cards to store and transport secure information. These rejections are respectfully disagreed with, and are traversed below.

The deficiencies of the '800 reference is discussed above.

The Applicant refutes the Examiner's taking of Official Notice, because the Examiner has provided no examples or evidence supporting the subject matter of the Official Notice. Claims, 10 and 15 depend directly from claims 9 and 11, respectively. Because claims 9 and 11 are asserted to be patentable for the reasons presented above, and because the Official Notice is unsubstantiated, dependant claims 10 and 15 are necessarily non-obvious and therefore patentable. Applicant, therefore, submits that claims 10 and 15 are allowable. Accordingly, Applicant respectfully requests that the rejections of claims 10 and 15 be reconsidered and withdrawn.

The Examiner rejects claim 14 under 35 U.S.C. §103(a) as being unpatentable over the '800 reference in view of U.S. Patent No. 5,613,012 to Hoffman (hereinafter the '012 reference). The Examiner states that the '800 reference does not disclose the sequence number being comprised of one of decreasing numbers, numbers with a step interval greater than unity and numbers representing date and time, the time including a number of seconds from an appointed start time. However, the Examiner alleges that the '012 reference teaches

the sequence number being comprised of one of decreasing numbers, numbers with a step interval greater than unity and numbers representing date and time, the time including a number of seconds from an appointed start time. The Examiner further alleges that it would have been obvious for one of ordinary skill in the relevant art to modify the '800 reference in view of the teachings of the '012 reference to arrive at the invention of claim 14. These rejections are respectfully disagreed with, and are traversed below.

The deficiencies of the '800 reference is discussed above.

The '012 reference is merely seen to disclose a method for authorization of transactions and transmissions. The method of the '012 reference discloses the use of a private code that is returned to a user after an identification is complete, thereby authenticating access to a computer system. The '012 reference discloses a unique transmission code having a unique hardware identification code and sequence number which increases by one for each transmission, rather than disclosing the sequence number being comprised of one of decreasing numbers, numbers with a step interval greater than unity and numbers representing date and time, the time including a number of seconds from an appointed start time, as recited in claim 14 of the present application. Claim 14 depends directly from claim 11. Because claim 11 is asserted to be patentable for the reasons presented above, and because the '012 reference does not cure the deficiencies of the '800 reference, dependant claim 14 is necessarily non-obvious and therefore patentable. Applicant, therefore, submits that claim 14 is allowable. Accordingly, Applicant respectfully requests that the rejection of claim 14 be reconsidered and withdrawn.

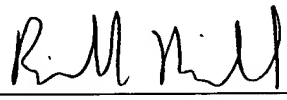
Applicant believes that the foregoing amendments and remarks are fully responsive to the Office Action and that the claims herein are allowable. In view of the foregoing points that distinguish Applicant's invention from those of the prior art and render Applicant's invention novel and non-obvious, Applicant respectfully requests that the Examiner reconsider the present application, remove the rejections, and allow the application to issue.

If the Examiner believes that a telephone conference with Applicant's attorneys would be advantageous to the disposition of this case, the Examiner is invited to telephone the undersigned.

Based on the foregoing and for at least these reasons, Applicant respectfully submits that claims of the application in question are in condition for allowance and an early action to that effect is earnestly solicited.

No fee is believed due with the filing of this Amendment. However, if a fee is due, Applicant authorizes the payment of any additional charges that may be necessary to maintain the pendency of the present application to the undersigned attorney's Deposit Account No. 503342.

Respectfully submitted,

By 

Richard R. Michaud
Registration No. 40,088
Attorney for Applicant

Michaud-Duffy Group LLP
CenterPoint
306 Industrial Park Road
Suite 206
Middletown, CT 06457-1532
(860) 632-7200